Technische Universität München, Department of Informatics

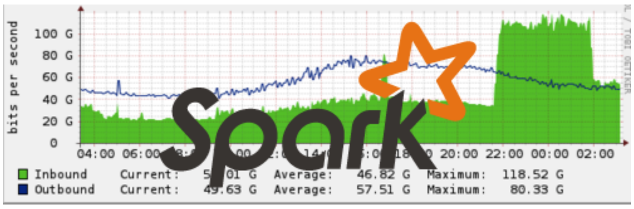
Chair for Network Architectures and Services
Prof. Dr.-Ing. Georg Carle

Thesis M.Sc.

IDP, Guided Research

Botnet Detection using Machine Learning on Flow Data

Motivation



Botnets are a major threat to the security of the Internet. The C&C servers send commands to the bots which then execute these commands and perform e.g. Distributed Denial-of-Service (DDoS) attacks, spam campaigns or scan for vulnerable hosts. In order to eliminate the threats posed by botnets it is necessary to detect C&C servers and infected hosts as participants in those botnets. Research shows [1, 3] that it is generally possible to automatically perform this detection in the network. In this thesis you will investigate the use of machine learning to detect botnet C&C connection. As machine learning framework we will use Apache Spark [2].

Your Task

- Extract and transform flow data to features for machine learning
- Explore and implement supervised and unsupervised models
- Evaluate feature and models for botnet detection

Requirements

- Knowledge in Scala, Java and/or Python
- Understanding of the concepts of flow data (IPFIX) and machine learning
- Willingness and motivation to experiment and learn new concepts autonomously (GIYF-based work approach)

Bibliography

[1] Leyla Bilge, Davide Balzarotti, William Robertson, Engin Kirda, and Christopher Kruegel. Disclosure: detecting botnet command and control servers through large-scale netflow analysis. In *Proceedings of the 28th Annual Computer Security Applications Conference*, pages 129–138. ACM, 2012.

[2] The Apache Software Foundation. MLlib — Apache Spark.

[3] Matija Stevanovic and Jesper Melgaard Pedersen. An efficient flow-based botnet detection using supervised machine learning. In *Computing, Networking and Communications (ICNC), 2014 International Conference on*, pages 797–801. IEEE, 2014.

Contact

Johannes Naab naab@net.in.tum.de
Oliver Gasser gasser@net.in.tum.de

https://www.net.in.tum.de/de/members/naab